*Library Acquisitions: Practice & Theory*, Vol. 18, No. 3, pp. 333-339, 1994.
ISSN: 0364-6408
http://www.sciencedirect.com/
http://www.sciencedirect.com/science/journal/03646408/18/3
http://dx.doi.org/10.1016/0364-6408(94)90017-5


ALCTS AUTOMATED ACQUISITIONS DISCUSSION GROUP
THE AUDIT TRAIL AND AUTOMATED ACQUISITIONS:
SEARCHING FOR ROAD SIGNS

# THE AUDIT TRAIL AND AUTOMATED ACQUISITIONS: SEARCHING FOR ROAD SIGNS

*CAROL PITTS HAWKS*

## INTRODUCTION

Most of my audit experience comes from an audit of the purchasing and payables functions of the Acquisition Department in 1987. This was the first audit since implementation of the INNOVACQ system in 1984. The audit was of particular importance to us because we are a satellite accounts-payable operation on campus. We issue our own purchase orders and are allowed to mail out our own checks though the checks are issued centrally [1]. As a result of that experience I did some research on the auditing process in the business literature. As a beginning, let me make three statements about auditing:

1. If you understand the concepts behind auditing and if you educate yourself just a bit, you can pass an audit without major problems.
   No one teaches us about auditing in library school. So it is imperative that you learn about this process on your own. Armed with that knowledge, examine your operation and correct any major problems with your organization, security, or automated system.
2. If you use an INNOVACQ Acquisitions System, you can pass an audit without major problems.
   I did a joint workshop at NASIG in 1992 with Sandy Weaver Westall of III. Sandy's part of that presentation was to discuss what a vendor does to ensure the integrity of their accounting functions. She focused particular attention on the importance of what many of us take for granted —that the system can add and subtract correctly and keep track of the integrity of every financial transaction. That is no small feat for a program, though most of us take that portion of our systems for granted.
3. Despite your best efforts, no automated acquisitions system will ever be secure enough for an auditor. An auditor must find something wrong to recommend for change during the audit.
   Auditing is really about risk. How much risk is the library or your institution willing to take? Some things are required, like separation of functions, which we shall discuss briefly later. However, because of budget constraints and the complexities of purchasing library materials, your

system will never be as secure as the auditor would prefer. Your parent institution will have requirements that must be met; you will have to determine how much risk to absorb in the "gray," less well defined areas.

OSU passed its audit with flying colors in 1987. However, the primary issues during that audit, which involved the automated acquisitions system, were password security and the segregation of functions, maintenance of signature files, and the retention of information. There were other minor nonautomated issues, but our focus is on the system issues.

## PASSWORD SECURITY AND SEGREGATION OF FUNCTIONS

Let me begin with password security and the segregation of functions by quoting directly from the Audit Report we received in 1987:

> ... we noted that 78 percent of the employees' system authorizations tested allowed access to INNOVACQ functions that are incompatible. ... By providing excess authorizations, the department creates an exposure to unauthorized or erroneous transactions [2].

Audit standards require the segregation of three functions: purchase order preparation, receiving, and invoice processing and payment. Although it is more difficult to ensure adequate segregation in a small organization, as long as the organization or department has at least three employees, segregation can be maintained. In essence, the person who placed the order should not be the person who receives it or the person who pays for it. In practice, this may seem relatively easy to achieve. Within an automated system it may become more difficult to achieve if the password structure is too flexible. For example, even though the staff member who issues orders may not be responsible for receiving material, if his password allows him to receive material (or even update the receipt date), segregation of functions has been violated.

Some individuals argue that systems are secure because staff members have not been "trained" or instructed in the procedure for something, even though their passwords allow it. That is a flawed argument in this context because the issue is what it is possible for staff members to do within the system, not what activities you have trained them to perform. We do not "train" anyone to perpetrate fraud by issuing payments to him/herself. Audit control requires our automated systems to prevent that fraud from occurring, not just to rely on the integrity of our employees.

At OSU, the auditors prepared the grid shown to illustrate the principles of segregation that they wished us to employ in our password structure (Table 1). The table includes the function, examples of appropriate tasks, and examples of inappropriate tasks. Much of this is relatively easy to secure. Even though the initial report indicated a 78% level of lax security, much of that was the result of failure on our part to review carefully and confine the password structure. Much of that was eliminated by reexamining the passwords for each person and confining them to specific tasks.

**TABLE 1**
UNIVERSITY LIBRARIES PROPOSED SYSTEM FOR TASK ALLOCATIONS*

This grid is to help segregate the job functions of the Department of Acquisition. To fully achieve the segregation needed, the department should have critical data fields in the update function protected.

| Process | Functions | Examples of appropriate tasks | Examples of inappropriate tasks | Comments |
|---|---|---|---|---|
| Ordering | Build records<br>Update records<br>Print PO<br>Merge Records<br>Cancel Records | Data Entry<br>Editing<br>Print PO<br>Claiming<br>Delete/change | Receive merchandise<br>Change vendor history<br>Process invoice | |
| Receiving | Check-ins | Receive merchandise | Change or delete order<br>Process invoices<br>Change vendors | Linited access to data-field should be considered. |
| Invoice processing | Process invoices<br>Build fund codes | Pay invoices<br>Establish fund codes<br>Generate financial reports | Change or delete order<br>Print PO<br>Receive merchandise | |
| File maintenance - Level I | Access vendor files<br>Backup files<br>System maintenance | Change vendor history<br>Backup files | Process order<br>Receive merchandise<br>Process invoice | Access should be listed to one person and supervisor or manager. |
| Level II | Access password files | Adding or removing individuals to password file | Process order<br>Receive merchandise<br>Process invoice | Access should be limited to managers. Also, manager should not be involved in the daily job activity. |

*The Ohio State University Libraries, 1987 — prepared by the University internal auditors

However, from our experience, the single greatest flaw in the security of the INNOVACQ system was the inability to segregate individual fields in the order record from update in the update function. For example, in the invoicing process, as noted on the chart, invoicing staff members should not be allowed to change an order. We wanted invoicing staff to have access to the update function for adding internal notes, vendor addresses, and changing acquisition types (thus, changing the order). By providing passwords that allowed them to perform these activities, the invoicer could also update order and receiving information such as receipt date (rdate) and order date (odate) —two of the key elements in the integrity of segregating the ordering, receiving, and invoicing processes.

To satisfy the auditors, we wrote a formal letter of request to Innovative Interfaces asking that the system be enhanced to provide better security. In addition, we limited update functions for invoicing activities to the supervisor of the accounting division rather than allowing the other three invoice processing staff members to have these capabilities. Unfortunately, this creates some other risks, since the accounting supervisor also has other capabilities in the financial function that should be highly secured.

A final unanticipated problem was the dial-access modem that was connected to the system and used for problem solving by III. The auditors recommended that "the dial-up modem should be off when not actively in use. When III wishes to access the system, permission should be granted by logging the request, giving the approximate time required, stating the service to be performed,

and, if approved, activating the modem. The log should be used to document routine problems with the system. The use of a dial-back modem should be considered." [3] A dial-back modem is one that allows access to a system by calling back the number of the person who placed a call originally. If III dialed into the system, the modem would verify their right to access the system and then "dial back" the system and allow the access. Initially, we did abide by this recommendation by unplugging the modem and requiring III to call us when they needed to access the system. We never considered this a serious audit risk (though the auditor did). I will confess that we became rather lax about leaving the modem unplugged as time went on.

**SIGNATURE FILE**

Most of you are probably familiar with the signature-file concept maintained by banks. When you open an account, you sign a signature card that is your official signature for comparison against checks, should the situation warrant. Anyone else who is authorized to write checks on your account will also be required to sign the card. These cards are not consulted every time we make a transaction at the bank, but they are the official authorization documents for your accounts.

One result of our audit in 1987 was the requirement that we maintain a signature file for every fund in our INNOVACQ system. We implemented this by maintaining a card for each collection manager which included the funds on which they were authorized to initiate purchases. After the card was completed, the manager was required to initial and sign the card much as we are required to sign signature cards at the bank. This requirement applies to every "order" placed by the Acquisition Department. In essence, the collection managers must authorize purchase of all order requests they submit; they must initial and add the fund to a flag that is inserted in each approval book that they select. In addition, when they submit approval notification slips for ordering, each slip must be individually initialled.

These authorizing initials are keyed into the INNOVACQ system as online documentation that the order was initiated by someone outside the Acquisition Department. Replicating this information in the online system is only for our information and use; the official documentation is the actual paper forms themselves. After the title is received, the paper order form with the official initials is filed in shoe-box-like files by receipt date. The University's Internal Audit Department argued that:

> The heart of the recommendation is not the document used, but your evidence prior to purchase that the transaction was authorized by a party independent of the Acquisitions Department [4].

As you might guess, we were patently opposed to this requirement, arguing that our collection managers recommended titles for purchase, while the Acquisition Department was the actual ordering authority. The University Archivist and the State Auditor concurred with the library stating that:

> It is not necessary to retain Form 15510 as part of an audit trail… if the other internal controls, such as receiving, cataloging, shelflist, etc. are adequate to

protect the financial integrity of the acquisitions process [5].

You might be surprised to learn that we lost this battle even with the State Auditor on our side. Basically, the University is entitled to be more stringent than the State and can enforce greater controls (as they did in this case). Obviously, they cannot be less stringent than the State but they can be more stringent.

Now, on this issue I have been talking exclusively about a manual solution to the signature file. I confirmed at the time of the audit that an electronic signature file would also suffice, though INNOVACQ did not have one at that time, nor do they have one at this point. Basically, an electronic signature file would be required in our case if collection managers were to be allowed to key their order requests directly into INNOVACQ rather than submitting paper forms. As a part of the system's password security, the collection manager would sign on with a password which would identify him to the system and allow him specific functions such as the ability to add new order requests but not initiate purchase orders. Each order record would automatically record and display the name of the password used to key the order. That field would be system-created and would not be updatable. In addition, the password system would go a step further and verify that the fund code added to the order was included in a list in the system for which the collection manager was authorized to make purchases. The system would not accept a fund code that was not authorized for the password being used.

At OSU we have been pursuing an enhancement of this type with III for the INNOVACQ system (although we have not yet convinced them to provide it). We believe it is imperative for streamlining and paper-file elimination to move forward with allowing our collection managers to key their orders directly into the INNOVACQ system. I am also convinced that this is doable, because it was a integral feature of at least one other automated acquisitions system as early as 1986 — the original Geac Acquisitions System.

## RECORDS RETENTION

Since the University Archives and its Archivist are members of the library faculty at OSU, we have been able to define record retention schedules for most operations in the libraries. As a result of the audit in 1987, the Acquisition Department's schedule was updated to include not only the new paper files generated by the INNOVACQ system but the electronic records as well. The electronic order record includes basic bibliographic information,' the person initiating the request, the PO number, the vendor, invoice information, fund accounting information, date of receipt, and date of payment. Our current schedule reads:

> Retain 5 years after payment, then destroy, provided that audit report of State Auditor has been released. (Record can be transferred from electronic to paper medium at any time but cannot be destroyed until 5 years after payment has been issued and audit report of State Auditor for the period has been released) [6].

At the time of this recommendation we were deleting records from our system on a regular basis onto paper files. Under our current configuration with INNOVACQ we are deleting these records to DAT tape. Because of storage limitations, we will delete and store these records on tape after approximately 18 months. Should an audit occur on these records after they are deleted, the tapes can be remounted and

accessed online on a title-by-title basis. They are not actually reloaded and indexed in the system, but are simply displayed in a workfile space for viewing and verification. After five years, the tapes can be discarded completely. In this regard, III has developed a very effective mechanism for meeting retention requirements while minimizing the online storage requirements and costs for libraries. Because we will be deleting a large set of records in the coming months as we prepare to implement the INNOPAC online catalog portion of the III system, we will delete material in categories such as gifts, theses, and paid titles. Each type of material will be stored on individual tapes. Also, the deleted records will occur on particular dates so that the type of material deleted and its location will be easier to find and reload.

Two additional financial files that are part of the III system are created in paper format and must be retained in that fashion: the posting register and the fund ledgers. The posting register is created by INNOVACQ as a chronological listing of all payments to vendors and includes the name of the vendor, the invoice number and date and the purchase order number, and any disencumbrances. This paper documentation is created every time that the financial files are updated through a program known as "posting." We post twice a day, so the amount of paper created is substantial. These documents are kept in chronological order in notebooks throughout the current year for ready reference. They are retained in this format for five years and then destroyed [7], The second file, the fund ledgers, are paper records that show budget transfers and cash rollovers in each fund used to buy library materials. This file does not include information about individual purchases of library materials [8]. I would much prefer that these audit trails were maintained in an online fashion. In their current paper formats, they are more difficult to use and less accessible than they would be online.

## CONCLUSION

As I have indicated above, our audit found the Acquisition Department process to be very clean. We lost one battle about the retention of the paper order forms from collection managers. The password file was tightened as much as possible at the time, though I expect an audit of it today would find that some laxity has once again crept in. The final communication from the Internal Audit Department reveals what I mentioned earlier, that a certain level of risk can be tolerated:

> The department has taken action to correct incompatible job functions noted during the audit by limiting employees' access to as few functions as possible without impeding departmental operations. However, additional access restrictions cannot be made because the INNOVACQ system is unable to restrict access to data fields in the update function. We understand that the vendor has been contacted to rectify the system weaknesses, but to no avail. Therefore, the department has opted to accept the risk of operating with the current system until the vendor can be persuaded to develop the specific enhancements [9].

## NOTES

1. Hawks, Carol Pitts. "Internal Control, Auditing, and the Automated Acquisitions System," *The Journal of Academic Librarianship* 16 (1990), 296-301.
2. The Ohio State University, University Libraries, Audit Report dated February 3, 1988, pp. 2-3.
3. Ibid., p. 3.
4. Letter from Deborah Maldonado, Acting Director, Internal Audit, The Ohio State University, to William J. Studer, Director for Libraries, dated March 9, 1988.
5. Letter from Raimond E. Goerler, University Archivist, The Ohio State University, to Carol Hawks, Head, Acquisition Department, dated February 12, 1988.
6. Records Retention Schedule for the Acquisition Department, University Libraries, The Ohio State University, dated May 13, 1988, p. 1.
7. Ibid., p. 2.
8. Ibid.
9. Letter from Gary N. Jones, Internal Audit, The Ohio State University, to William J. Studer, Director of Libraries, dated November 18, 1988.